IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
EL PASO DIVISION

UNITED STATES OF AMERICA,	**§**	
	§	
Plaintiff,	**§**	
v.	**§**	**Cause No.: EP-11-CR-2728-KC**
	§	
ANGEL OCASIO,	**§**	
	§	
Defendant.	**§**	

GOVERNMENT'S AMENDED NOTICE OF EXPERT AND MEMORANDUM OF LAW

TO THE HONORABLE JUDGE OF THE UNITED STATES DISTRICT COURT:

COMES NOW the United States of America, by and through the United States Attorney for the Western District of Texas and the undersigned Assistant United States Attorneys, and files this Notice of Expert and would show unto the Court the following:

Defendant Angel Ocasio is charged in a four-count Indictment charging various violations relating to the receipt, distribution and possession of child abuse images. Trial currently is scheduled for jury selection on June 21, 2013.

Pursuant to Federal Rule of Criminal Procedure 16(a)(1)(E) and the Court's Order of June 13, 2013 [ECF Doc. 158], the Government hereby files it's Amended Notice of Expert that the following persons may be called as an expert at trial in this case:

1) **Sergeant Matthew Pilon, New Mexico State Police, Online Predator Unit.**

   Sergeant Pilon will provide the jury with an overview of the how peer-to-peer software operates and facilitates the nearly anonymous trading of digital files, including those that contain images of children

engaged in sexually explicit activity, via the Internet. A copy of his demonstrative powerpoint previously was supplied to defendant and summary of his testimony is attached hereto as Exhibit A.

Sergeant Pilon previously has testified as an expert witness in federal district court. A copy of his Curriculum Vitae is attached hereto as Exhibit A-1.

2) **Demetrio Medina, Computer Forensics Agent, Department of Homeland Security, Homeland Security Investigations, CyberCrimes Group.**

Agent Medina will testify as to the child sexual abuse images found on digital media belonging to defendant and the manner in which such was discovered. A full copy of the agent's report setting forth his actions and findings, the Forensic ToolKit Report, various supplemental emails, and screenshots hav been supplied to counsel in discovery; a further summary of his testimony is attached hereto as Exhibit B.

Agent Medina previously has testified as an expert witness in federal district court. A copy of his Curriculum Vitae is attached hereto as Exhibit B-1.

3) **Joseph Byers, Computer Forensics Agent, Department of Homeland Security, Homeland Security Investigations, CyberCrimes Group.**

If called, Agent Byers will testify where specific items of computer equipment were located in the defendant's bedroom and the imaging conducted on EXT1. A full copy of the forensic report detailing his actions and findings has been supplied to counsel in discovery and is repeated via a summary of his testimony attached hereto as Exhibit C.

Agent Byers previously has testified as an expert witness in federal district court. A copy of his Curriculum Vitae is attached hereto as Exhibit C-1

The witnesses will be testifying primarily as to factual matters and it is not anticipated they will be asked to render an opinion during direct examination; however, as these witnesses will be testifying from specialized knowledge and training, this Notice is being filed.

The admissibility of expert opinion testimony generally turns on the following preliminary question of law determinations by the trial judge under Federal Rules of Evidence, Rule 104(a):

- Whether the opinion is based on scientific, technical, or other specialized knowledge, Fed. R. Evid 702;

- Whether the expert's opinion would assist the trier of fact in understanding the evidence or determining a fact in issue, Fed. R. Evid 702;

- Whether the expert has appropriate qualifications, that is, some special knowledge, skill, experience, training, or education on that subject matter, Fed. R. Evid 702; *Jones v. Lincoln Elec. Co.*, 188 F.3d 709 (7th Cir. 1999); *See Wilson v. Woods*, 163 F.2d 935, 936 (5th Cir. 1999)(expert in fire reconstruction unqualified as expert in auto accident reconstruction).

- Whether the testimony is relevant and reliable. *Daubert v. Merrell Dow Pharmaceuticals*, *Inc.*, 509 U.S. 579, 589 (1993); *Kumbo Tire Company, Ltd. v. Carmichael*, 526 U.S. 137, 152-53 (1999).

- Whether the methodology or technique the expert uses "fits" the conclusions (the expert's credibility is for the jury). See *General Electric Co. v. Joiner*, 522 U.S. 136, 145 (1997);

- Whether its probative value is substantially outweighed by the risk of unfair prejudice, confusion of issues, or undue consumption of time. Fed. R. Evid. 403.

The Fifth Circuit reviews a district court's determination of admissibility of expert testimony under an abuse of discretion. *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993).

WHEREFORE, premises considered, the United States requests, should it elect to call the above-referenced individual, that he be designated as an expert witness, if necessary, in the instant case.

Respectfully submitted,

ROBERT PITMAN
UNITED STATES ATTORNEY

By: /s/

J. BRANDY GARDES
Assistant United States Attorney
CA Bar No. 144770

/s/
DANIEL R. CRUMBY
Assistant United States Attorney
TX Bar No. 24049839
700 E. San Antonio, Ste. 200
El Paso, Texas 79901
(915) 534-6884

CERTIFICATE OF SERVICE

I hereby certify that on the 14th day of June, 2013, a true and correct copy of the foregoing instrument was electronically filed with the Clerk of the Court using the CM/ECF System which will transmit notification of such filing to the following CM/ECF participant:

Michael Gorman, Esq. — Attorney for Defendant
Shane McMahon, Esq.
Federal Public Defenders Office
700 E. San Antonio, 4th Floor
El Paso, Texas 79901

/s/
J. BRANDY GARDES

EXHIBIT A
SUMMARY OF TESTIMONY EXPECTED FROM MATTHEW PILON

Sergeant Matt Pilon will testify that as part of his training and experience, he is familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use the Internet must first obtain an account linking it to the Internet – for example, through a commercial service – which is called an "Internet Service Provider" or "ISP" (see definition of "Internet Service Provider" below).

Domain Name

He will testify how computers connect to the Internet through the use of domain names. Domain names are common, easy to remember names associated with an Internet Protocol address (defined below). For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. When a user types in the domain name of a website he or she wants to view in an Internet browser, a request is sent from the user's computer to the sever that is hosting the website. Once that request is received by the server, the server provides a "response" and completes the basic cycle that makes websites work: the browser makes a request, the server processes that request, including accessing any images and returns the appropriate response to the browser.

Internet Service Providers (ISPs) and the Storage of ISP Records:

Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of services for their customers including access to the Internet. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish

communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers.

Internet Protocol Address (IP Address)

Typically, computers or devices on the Internet are referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records.

Peer to Peer File Sharing

Sergeant Pilon will educate and demonstrate how peer to peer programs operate and how they are used to share images and pictures. Peer to peer file sharing is a free open source software process that allows computer users, utilizing the same file sharing software, to connect to each other and directly access files from one another's computer hard drive. He will describe how one computer can connect to numerous other computers in order to receive images and videos. The software only allows remote users to access shared folders. Some examples of peer to peer files sharing software are Frostwire, Napster, Kazaa, Grokster, Gnutella, eMule, Morpheus, Phex, etc.

Frostwire was located on C1H1. In particular, he will discuss how Frostwire 4.21.8 connects to the Gnutella network.

He will walk the jury through the Frostwire installation process and the disclaimer process. The disclaimer informs users that they are using a file sharing program and the user must click "I Agree" in order to continue the installation process. The installation allows the user to select the installation destination on the computer. Once the installation is selected the user must select "Next" to continue with installation. The user then elects to install RealPlayer to play and view the images and videos. Finally, the user must check the box to "Run Frostwire" and select finish to start the Frostwire program.

Next the user has to complete the Frostwire Setup Wizard. The first step is to determine the "save" and "shared" folders on the users computer. The user has the ability to share all of his folders and subfolders, share some folder files and subfolders, or share none of his folders and subfolders. The user has to check a box to make the election to share or not share. Further, if the user elects to share, the user must designate which folders to share. The user clicks next to move to the next setup screen.

The user is allowed to select their network speed for their internet service and whether Frostwire will startup automatically when the user logs into the computer. The user is prompted to make some adjustments to their firewall in order to Frostwire to share and receive files. Next the user is prompted to designate which file extensions and file types to share such as audio, documents, images, programs, torrents, video and other. Lastly, users receive a notice about using Frostwire for authorized purposes and prompting the user to agree not to use the program for copyright infringement.

Next, the program opens and the user is able to search for images and videos. Users must input search terms into the search box and click search so that Frostwire can locate the image and videos the user seeks. This is called a "keyword" search. The results of the search are displayed and the user selects which files they want to download by clicking on the file name.

Once a file has been downloaded, it is stored in the area previously designated by the user. The user can view the images and videos they downloaded by clicking on the file name. Files that are downloading are located in the "queue" accessible under the download tab. When these files are downloading, the user has the option to stop the download and to remove the file. If the user does not stop the download and/or remove the file, the file is stored in the shared folder previously setup by the user.

Frostwire has a tab for "My Shared Files" which tells users which files they are sharing. In the bottom corner of the program is an indicator which informs users that they are sharing files and which files they are sharing.

SHA1 (Secure Hash Algorithm)

He will explain how file sharing programs use algorithms for computing a 'condensed representation' of a message or a data file. The 'condensed representation' is of fixed length and is known as a 'message digest' or 'fingerprint'. These algorithms are useful in that it is conjectured that it is computationally infeasible to produce two messages having the same message digest. This uniqueness enables the message digest to act as a 'fingerprint' of the message opening up the possibility of using this technology for issue like data integrity and comparison checking. For instance when one downloads or receives a file, one can use SHA-1

to guarantee that you have the correct, unaltered file by comparing its hash with the original, which verifies the file's integrity.

Matthew Pilon

4491 Cerrillos Road• Santa Fe, New Mexico 87507
Phone: 505 827-9066 • Fax: 505 827-9063 • E-Mail: matthew.pilon@state.nm.us

Employment

New Mexico State Police January 2009 to Present

Sergeant assigned to On-line Predator Unit

New Mexico State Police September 2009 to January 2009

Acting Sergeant assigned to On-line Predator Unit

New Mexico State Police April 2007 to September 2009

Agent assigned to Investigations On-line Predator Unit

New Mexico State Police June 2001 to April 2007

Patrol Officer assigned to District 1, Santa Fe and Pecos

United States Army June 1990 to June 1994

Enlisted Military Police

Education

New Mexico State Police Recruit School, Santa Fe, NM June 2001

Graduated State Police Officer

Lake Superior State University May 1998

Bachelor of Science in Criminal Justice

United States Army October 1990

Graduated Military Police School

Training

- **385 hours Computer Forensic Training**
- **336 hours Child Abuse Investigations**
- **1572 hours Law Enforcement training**

2011

State of New Mexico, Department of Public Safety, In-service Training, 23 hours, Santa Fe, NM, November 16, 2011

Mentor Forensic Services, Internet & Technology Facilitated Sexual Exploitation of Children, 16 hours, Boca Raton, FL, November 7-8, 2011

State of New Mexico, Department of Public Safety, Instructor Development, 40 hours, Santa Fe, NM, October 17-21, 2011

State of New Mexico, Department of Public Safety, Self Determination, OLC, 16 hours, Santa Fe, NM, October 14, 2011

EnCE Certified Examiner, certification number 15-0911-4323, September 13, 2011

CEIC, Computer and Enterprise Investigations Conference, -12 hours - Orlando, FL May 15-18, 2011

State of New Mexico, Department of Public Safety, Firearms Instructor - Rifle, 40 hours, Albuquerque, NM, May 9-13, 2011

State of New Mexico, Department of Public Safety, Firearms Instructor - Handgun, 56 hours, Albuquerque, NM, April 25 – May 3, 2011

TLO Corporation, Beyond Fairplay – Instructor update – 20 hours – Boca Raton, FL January19-21, 2011

2010

Broward County Sherriff's Office, Basic Gigatribe Investigations, 12 hours, Boca Raton, FL November 4-5, 2010

Black Bag Technologies, Introduction to Mac Forensics, 35 hours, Reston VA, September 22 to October 1, 2010

Dallas Children's Advocacy Center, 22nd Annual Crimes Against Children Conference, 19.5 hours, Dallas TX, August 9-12, 2010

United States Department of Justice, ICAC RoundUp Training Program, 12 hours, Albuquerque, NM August 2-3, 2010

Access Data, Mac Forensics, 21 hours, Santa Fe, NM, April 13-15, 2010

Access Data, Windows Forensics Registry, 21 hours, Santa Fe, NM, February 9-11 2010

Access Data, Bitpim & Cellular Phone Artifacts, 7 hours, Santa Fe, NM, February 5, 2010

Access Data, Internet Forensics, 21 hours, Santa Fe, NM, January 12-14, 2010

2009

State of New Mexico, Department of Public Safety, In-service Training, 41 hours, Santa Fe, NM, December 16, 2009

State of Nebraska, Department of Justice, Operation Fairplay – Instructor Development Course, 24 hours, Boca Raton, FL, November 9-11, 2009

Access Data, Windows Forensics Vista, 21 hours, Santa Fe, NM, September 15-17, 2009

Access Data, Access Data Forensics, 35 hours, Santa Fe, NM, August 31- September 4, 2009

2008

United States Department of Justice, Specialized Strategies in Child Abduction Cases, 36 hours, Albuquerque, NM. November 17-21, 2008

United States Department of Justice, Project Safe Childhood National conference, 21 hours, Columbus, OH. September 23-26, 2008

Sam Houston State University, Advanced Digital Forensics Concepts, 40 hours, Houston, TX. August 4-8, 2008

United States Department of Justice, Project Safe Childhood Team Training, 36 hours, Albuquerque, NM. June 2-6, 2008

State of Wyoming, Division of Criminal Investigation, Operation Fairplay, 28 hours, Cheyenne, WY. March 21 – April 2, 2008

State of New Mexico, Department of Public Safety, First Line Supervisor Training, 40 hours, Santa Fe, NM, April 4, 2008

Guidance Software, EnCase Computer forensics II Course, 32 hours, Pasadena, CA. February 26 – 29, 2008

SEARCH, The National Consortium for Justice information and Statistics, Advanced Responders –Search and Seizure of SOHO Networks, 24 hours. Little Rock, AR. February 12-14, 2008

State of New Mexico, Department of Public Safety, Domestic Violence, 4 hours, Santa Fe, NM, February 5, 2008

State of New Mexico, Department of Public Safety, Critical Incident Management, 16 hours, Santa Fe, NM, February 1, 2008

2007

National White Collar Crime Center, Cyercop 201 IDRA, Intermediate Data Recovery and Analysis, 36 hours, Albuquerque, NM. December 10-14, 2007

State of New Mexico, Department of Public Safety, In-service Training, 24 hours, Santa Fe, NM, November 5-9, 2007

SEARCH, The National Consortium for Justice information and Statistics, ICAC Core Skills for the Investigation of Cellular Telephones, 32 hours. Las Vegas, NV. November 13-16, 2007

State of New Mexico, Department of Public Safety, The Bullet Proof Mind, 8 hours, Santa Fe, NM, November 2, 2007

United States Department of Justice, ICAC Undercover Chat Training Program, 36 hours, Overland Park, KS. September 17-21, 2007

United States Department of Justice, ICAC Investigative Techniques Training Program, 36 hours, Colorado Springs, CO. June 11-15, 2007

New Mexico Attorney General's Office, Foreign Prosecutions / Extraditions with Mexico & Consular Notifications, 8 hours, Santa Fe, NM. May 17, 2007

State of New Mexico, Department of Public Safety, Specialized Investigation of Sexual violence, 40 hours, Las Cruces, NM. May 7-11, 2007

National White Collar Crime Center, Cyber Investigations 101, STOP, Secure Techniques for Onsite Preview. 16 hours, Albuquerque, NM. February 26-27, 2007

National White Collar Crime Center, Cybercop 101 BDRA, Basic Data Recovery and Acquisition, 32 hours, Phoenix, AZ. January 8-11, 2007

2006

New Mexico Coalition of Sexual Assault Programs, Sexual Assault Investigation, 8 hours, Las Vegas, NM. November 2, 2006

State of New Mexico, Department of Public Safety, Background Investigations, 4 hours, Las Vegas, NM. October 26, 2006

John E. Reid and Associates, Child Abuse Investigations, 21 hours, Farmington, NM. January 24-26, 2006

2004

State of New Mexico, Department of Public Safety, In-service Training, 40 hours, Santa Fe, NM, October 4-8, 2004

John E. Reid and Associates, The Reid Technique of Interviewing and Interoogation, 21 hours, Las Vegas, NV. May 25-27, 2004

State of New Mexico, Department of Public Safety, Search Warrants and Confidential Informants, 16 hours, Santa Fe, NM. April 15, 2004

State of New Mexico, Department of Public Safety, Spanish Immersion, 40 hours, Santa Fe, NM. March 8-12, 2004

2003

State of New Mexico, Department of Public Safety, Sexual Harassment, 3 hours, Santa Fe, NM. July 10, 2003

2002

New Mexico National Guard, Vehicle Inspection Techniques, 8 hours, Taos, NM. August 15, 2002

State of New Mexico, Department of Public Safety, Sexual Harassment Training, 8 hours, Santa Fe, NM. March 28, 2002

2001

State of New Mexico, Department of Public Safety, State Police Recruit Training, 1087 hours, Santa Fe, NM. March 4 – June 22, 2001

Guest Lecturer and Instructor

- Instruct Beyond Fairplay – Basic P2P Investigation, Albuquerque, NM, February 21-24, 2012
- Instruct NMSP Academy – Technology Crimes, Santa Fe, NM, February 13, 2012
- Lecture at Protecting New Mexico from Child Exploitation Conference, Trading of Child Exploitation Images though the internet, and Crime Scenes involving Exploitation and Digital Evidence, Bernalillo, NM September 28-29, 2011
- Instruct Beyond Fairplay – Basic P2P Investigation, Santa Fe, NM, April 18-22, 2011
- Instruct Beyond Fairplay – Basic P2P Investigation, Albuquerque, NM, March 22-26, 2010
- Instruct Beyond Fairplay – Basic P2P Investigation, Phoenix, AZ, November 2-6, 2009
- Instruct Beyond Fairplay – Basic P2P Investigation, Phoenix, AZ, November 9-13, 2008

Expert Testimony In Federal Court

- *United States v. Patrick Railsback:* recognized as an expert in computer forensic examinations in Case No. 09-CR-2629 BB (United States District Judge Bruce Black).
- *United States v. Ethan Nathaniel Larman*: recognized as an expert in peer-to-peer software and undercover computer investigations *, No.* EP-11-Cr-1007-KC (United States District Judge Kathleen Cardone, Western District of Texas).

EXHIBIT B
SUMMARY OF TESTIMONY OF DEMETRIO MEDINA

During the execution of the Search Warrant, Special Agent/Computer Forensics Agent (SA/CFA) Demetrio Medina Jr., conducted a forensics preview of a Dell Dimension 2400 computer tower belonging to Angel OCASIO. SA/CFA Medina utilized a Tableau write protection device to connect the hard disk drive from the laptop to a CCG Computer Forensics laptop. The purpose of the Tableau write protection device is to prevent alteration of the suspect media. SA/CFA Medina then utilized Encase (version 6.19), a commercially available examination software application, to conduct the forensics preview. During the forensics preview, SA/CFA Medina found video files depicting images of child sexual exploitation (child pornography).

The preview was terminated and the computer was seized as well as other computers and various items of digital media, as follows:

1. A Dell computer tower (CPU) that was found in Bedroom 3, Room 9 (OCASIO's bedroom), designated and hereinafter referred to as C1, is identified as:

   Manufacturer: Dell
   Model: Dimension 2400
   Serial Number: 4S0QS31

   A single hard disk drive (HDD) was located within C1. The HDD was an Integrated Drive Electronics (IDE) device. The HDD, designated and hereinafter referred to as C1H1, is identified as:

   Manufacturer: Western Digital
   Model: WD400EB-75LPF0
   Serial Number: WMAATF728051
   Capacity: 40 Gigabytes (GB)

   The operating system was Windows XP Home Edition. CFA Medina is expected to testify as to what a hard drive is and it's function.

2. A Western Digital MyBook external hard disk drive, found in Bedroom 3, Room 9 (OCASIO's bedroom), designated and hereinafter referred to as EXT1, is identified as:

   Manufacturer: Western Digital
   Model: MyBook
   Serial Number: WCAU46252472
   Capacity: 1 Terabyte (TB)

3. A Dell computer desktop found in the living room Room 1, designated and hereinafter referred to as C2, is identified as:

Manufacturer: Dell
Model: Optiplex GX240
Serial Number: JCYLC11

A single HDD was located within C2. The HDD was an IDE device, designated and hereinafter referred to as C2H1, which is identified as:

Manufacturer: Maxtor
Model: 2B020HL
Serial Number: B1FD150E
Capacity: 20 GB

4. A Dell computer tower, designated and hereinafter referred to as C3, is identified as:

Manufacturer: Dell
Model: Optiplex GX260
Serial Number: GXFFY21

A single hard disk drive was located within C3. The HDD was an IDE device. The HDD, designated and hereinafter referred to as C3H1, is identified as:

Manufacturer: Western Digital
Model: WD400BB-75DEA0
Serial Number: WMAD19582578
Capacity: 40 GB

Acquisition

On October 7, 2011, SA/CFA Medina recorded the date/time settings from the Basic Input Output System (BIOS) of C1. The date/time recorded from the BIOS was October 7, 2011 / 13:46:00 hours Mountain Standard Time (MST). The actual time according to the United States Naval Observatory Atomic Clock website was October 7, 2011 / 13:46:02 hours MST. This indicates that date and time stamps on files located within the computer are accurate within 2 seconds.

SA/CFA Medina initiated imaging of C1H1. A forensic duplicate of C1H1 was created utilizing AccessData's Forensic Tool Kit (FTK) Imager, a commercially available forensic software program. The hard disk drive, C1H1, had the name "Angel Ocasio" written on it with permanent marker.

The imaging was conducted on a SAC El Paso CCG Computer Forensics Mac Pro computer utilizing a Tableau IDE write protection device to acquire hard disk drive images. The purpose of the Tableau write protection device is to prevent alteration of the suspect media.

To insure the integrity of the acquisition, a Message Digest 5 (MD5) hash value was calculated and obtained after the image was acquired. The purpose of calculating an MD5 hash value is to establish a functionally unique electronic signature of the data. The resulting hash value was recorded and matched a verification hash calculated subsequent to the acquisition.

FTK Imager returned the following hash value for C1H1.

C1H1: caad6908db4e8c834d2e3a1f804e803f
Evidence Files: C1H1-EP07QR11EP001.E01

C2H1

On October 20, 2011, SA/CFA Medina recorded the date/time settings from the BIOS of C2. The date/time recorded from the BIOS was October 20, 2011 /10:42:17 hours MST. The actual time according to the United States Naval Observatory Atomic Clock website was October 20, 2011 / 10:42:00 hours MST. This indicates that date and time stamps on files located within the computer are accurate within 17 seconds.

SA/CFA Medina initiated imaging of C2H1. A forensic duplicate of C2H1 was created utilizing FTK Imager.

The imaging was conducted on a SAC El Paso CCG Computer Forensics FRED computer utilizing a Tableau Ultrabay write protection device.

To insure the integrity of the acquisition, a MD5 hash value was calculated and obtained after the image was acquired. The resulting hash value was recorded and matched a verification hash calculated subsequent to the acquisition.

FTK Imager returned the following hash value for C2H1

C2H1: 1ed0df5c5511bf57d921788c80015079
Evidence Files: C2H1-EP07QR12EP0001.E01 through C2H1-EP07QR12EP0001.E08

C3H1

On October 20, 2011, SA/CFA Medina recorded the date/time settings from the BIOS of C3. The date/time recorded from the BIOS was October 20, 2011 /11:49:49 hours MST. The actual time according to the United States Naval Observatory Atomic Clock website was October 20, 2011 / 11:48:30 hours MST. This indicates that date and time stamps on files located within the computer are accurate to within 1 minute and 19 seconds.

SA/CFA Medina initiated imaging of C3H1. A forensic duplicate of C3H1 was created utilizing FTK Imager.

The imaging was conducted on a SAC El Paso CCG Computer Forensics FRED computer utilizing a Tableau Ultrabay write protection device to acquire hard disk drive images. The purpose of the Tableau write protection device is to prevent alteration of the suspect media.

To insure the integrity of the acquisition, a MD5 hash value was calculated and obtained after the image was acquired. The resulting hash value was recorded and matched a verification hash calculated subsequent to the acquisition.

FTK Imager returned the following hash value for C3H1.

C3H1: c89e53dc129535df3d86d96c6c240a6e
Evidence Files: C3H1-EP07QR12EP0001.E01 through C3H1-EP07QR12EP0001.E20

Examination

An examination of the contents of C1H1, EXT1, C2H1, and C3H1 was conducted by SA/CFA Medina utilizing AccessData's Forensic Tool Kit (FTK) (version 3.04.2138), a commercially available examination software application.

SA/CFA Medina opened FTK and added the aforementioned evidence files to new case EP07QR12EP0001. This process allowed the examination to proceed without altering any of the original files.

SA/CFA Medina initiated the examination by processing the case with FTK and examining those files which the software recognized as being of possible evidentiary value by virtue of their MD5 hash values matching previously encountered images and videos which are suspected of being child pornography.

The Department of Homeland Security hash set is comprised of hashes received from various state and local agencies, Federal agencies and independent organizations such as the National Center for Missing and Exploited Children (NCMEC); these are commonly referred to as "KFF" or "Known File Filter." SA/CFA Medina also visually examined all images and videos contained in the file structure.

C2H1 and C3H1

A search of both C2H1 and C3H1 were negative for the presence of videos or pictures depicting child pornography.

C1H1

FTK identified 2 video files from C1H1 which had been previously identified in other investigations as being images depicting child pornography. In EXT1, FTK identified 76 video files which had been previously identified in other investigations as being images depicting child pornography.

A further review of video files located on C1H1 and EXT1 was conducted utilizing the Overview tab within FTK. In C1H1, a total of 11 video files were located that are suspected of depicting child pornography. In EXT, a total of 96 video files were located that are suspected of depicting child pornography.

A listing of these videos was compiled and exported to the FTK Report.

The following is a description of one a video of child pornography from C1H1.

> Name: T-711968772-Russian Lolita 13 JOs-SaMix (PTHC)(R@y gold).mpg (Note: This file name is an abbreviation of the actual file name, due to the fact that the original file name contains foreign language characters.)
> File Extension: .mpg
> File Type: Moving Pictures Experts Group (MPEG)
> File Category: video
> File Created: 4/14/2011 9:48:34 PM (2011-04-15 03:48:34 UTC)
> Last Modified: 4/15/2011 12:58:52 AM (2011-04-15 06:58:52 UTC)
> Last Accessed: 8/10/2011 10:57:11 AM (2011-08-10 16:57:11 UTC)
> Evidence File: C1H1-EP07QR12EP0001.E01
> Full Path: C1H1-EP07QR12EP0001.E01/Partition 2/NONAME [NTFS]/[root]/Program Files/Incomplete/T-711968772- Russian Lolita 13 JOs-SaMix (PTHC)(R@y gold).mpg
>
> The video file, T-711968772-Russian Lolita 13 JOs-SaMix (PTHC)(R@y gold).mpg, is a video which consists of a compilation of 6 different video clips, all of which contain prepubescent females and adult males engaging in several sexual acts.

The files were found in the incomplete file but were able to be opened and viewed.

The following is a description of one of the videos depicting child pornography from EXT1.

> Name: Vicky - (Pthc) The 107 Minutes Collection.mpeg
> File Extension: .mpeg
> File Type: MPEG
> File Category: Video
> File Created: 5/29/2009 8:28:08 PM (2009-05-30 02:28:08 UTC)
> Last Modified: 5/28/2009 3:11:50 PM (2009-05-28 21:11:50 UTC)
> Last Accessed: N/A
> Evidence File: EXT1-EP07QR12EP0001.E01
> Full Path: EXT1-EP07QR12EP0001.E01/Partition 1/VIA LACTEA [FAT32]/[root]/NeroVision/DivX Movies/Ambient/New Limewire/Deuce/New Folder/Vicky - (Pthc) The 107 Minutes Collection.mpeg

> The video file, Vicky - (Pthc) The 107 Minutes Collection.mpeg, is a video compilation of different video clips depicting a prepubescent female engaged in sexual activities with an adult male.

A review of C1H1 utilizing FTK's Explore function showed that the peer to peer (P2P) file sharing program, Frostwire, was installed on this computer.

A review of the installation.props file for Frostwire, indicates that the latest version of the program, was installed on June 29, 2011. FTK indicates that both of these files were created on February 2, 2011. A review of the frostwire.props file for Frostwire, indicates that the peer to peer program was set to share and both were created through the "Owner" profile, which has a unique SID identifier of 1003.

The SAM file for the Owner account shows:

> Last successful logon: 10/6/2011 3:01:53 AM
> Last Password Change Time: 5/27/2011 5:46:21 AM
> Last Failed Logon Time: 10/6/2011 4:43 AM
> Account was not disabled

A review of the Owner account NTUSER.DAT file showed one of the recent files accessed via Windows Explorer was: (PTHC Pumped Girl 11 or 12 Enjoys Nice Sex {33m52S].mpg, which is a know "Vicky series" video.

A clone of C1H1 which was installed into Ocasio's computer show a password was required to login. The Owner profile further showed he had the folder options set to view or show hidden files and folders. The owner account was logged into 1097 times.

The last logon for the Guest account was on 8/14/2011 at 11:14. It had been logged onto 129 times. The profile further showed the folder options were set to not show or view hidden files and folders.

No other accounts listed on the profile had been logged into.

FINDINGS:

A list of items of interest located on C1H1 and EXT1, were prepared in FTK and supplied to the defendant. In C1H1, a total of 11 videos suspected of depicting images of child sexual exploitation were found.

In EXT1, a total of 96 videos suspected of depicting images of child sexual exploitation were found.

Both C1H1 and EXT1 were found in the bedroom occupied by OCASIO.

A comparison of the hash values for the videos located during the CPS scan and those found on C1H1 and/or EXT1, once converted to MD5 hash values, showed at least 14 videos seen by CPS were located on EXT1.

Personal documents belonging to OCASIO were found both on EXT1 and C1H1:

Name	Item #	Path	Category	Created	Accessed	Modified
Angel Ocasio Urinary System.docx	17663	C1H1-EP07QR12EP0001.E01/Partition 2/NONAME [NTFS]/[root]/Documents and Settings/Owner/My Documents/Angel Ocasio Urinary System.docx	Microsoft Word 2007	12/16/2010 1:15:52 AM (2010-12-16 08:15:52 UTC)	7/27/2011 10:38:49 AM (2011-07-27 16:38:49 UTC)	12/16/2010 8:42:58 PM (2010-12-17 03:42:58 UTC)
Ocasio Angel References.rtf	20425	C1H1-EP07QR12EP0001.E01/Partition 2/NONAME [NTFS]/[root]/Documents and Settings/Owner/My Documents/Ocasio Angel References.rtf	Microsoft RTF	11/19/2010 12:01:49 AM (2010-11-19 07:01:49 UTC)	9/22/2011 4:04:56 PM (2011-09-22 22:04:56 UTC)	11/19/2010 1:25:04 AM (2010-11-19 08:25:04 UTC)
Resume Angel Ocasio.rtf	379964	EXT1-EP07QR12EP0001.E01/Partition 1/VIA LACTEA [FAT32]/[root]/Word/Resume Angel Ocasio.rtf	Microsoft RTF	6/4/2009 10:39:42 PM (2009-06-05 04:39:42 UTC)	n/a	11/7/2010 2:37:10 PM (2010-11-07 21:37:10 UTC)
Texas Dept of Public Safety.rtf	20471	C1H1-EP07QR12EP0001.E01/Partition 2/NONAME [NTFS]/[root]/Documents and Settings/Owner/My Documents/Word/Texas Dept of Public Safety.rtf	Microsoft RTF	11/14/2010 10:37:48 AM (2010-11-14 17:37:48 UTC)	7/28/2011 1:09:26 PM (2011-07-28 19:09:26 UTC)	11/15/2010 11:06:25 PM (2010-11-16 06:06:25 UTC)
William Beaumont ArmyMC Cover Letter.rtf	379937	EXT1-EP07QR12EP0001.E01/Partition 1/VIA LACTEA [FAT32]/[root]/Word/William Beaumont ArmyMC Cover Letter.rtf	Microsoft RTF	9/24/2009 1:12:57 PM (2009-09-24 19:12:57 UTC)	n/a	12/8/2009 12:41:58 AM (2009-12-08 07:41:58 UTC)

Curriculum Vitae

Demetrio Medina Jr.
Special Agent
Computer Forensics Agent

Office Information

Department of Homeland Security
Immigration and Customs Enforcement
Homeland Security Investigations
Special Agent in Charge El Paso
4191 N. Mesa, Room 219
Employment Date: 03/11/2002

Education

University of Texas at El Paso
El Paso, Texas

Bachelors of Liberal Arts – Criminal Justice

Professional Training

Federal Law Enforcement Training Center
Criminal Investigator Training Program
2002

Federal Law Enforcement Training Center
Customs Basic Enforcement School
2002

Federal Law Enforcement Training Center
Prerequisite Computer Evidence Recovery Training (PCERT)
Vendor: Treasury Computer Forensics Training Program
Certificate Awarded September 28, 2006

Federal Law Enforcement Training Center
Basic Computer Evidence Recovery Training (BCERT)
Vendor: Treasury Computer Forensics Training Program
Certificate Awarded September 28, 2006

Federal Law Enforcement Training Center
CompTIA A+ Certified Professional
Certification Date: September 9, 2006
Certifying Authority: Computer Technology Industry Association

Paraben Certified Handheld Examiner Training
Vendor: Paraben Corporation
June 2008

ICE Cyber Crimes Center
Mobile Forensics (MFI 101) Training
Vendor: Mobile Forensics, Inc.
June 2008

ICE Cyber Crimes Center
Mobile Forensics (MFI 202) Training
Vendor: Mobile Forensics, Inc.
July 2008

AccessData Certified Examiner Training
Vendor: AccessData
August 2008 and August 2010

ICE Cyber Crimes Center
Advanced Computer Evidence Recovery Training Course (ACERT 1001)
Vendor: Treasury Computer Forensics Training Program
May 2010

Professional Certifications

CompTIA A+ Certification
Certification Date: September 9, 2006
Certifying Authority: Computer Technology Industry Association

Paraben Certified Handheld Examiner
Certification Date: June 20, 2008
Certifying Authority: Paraben Corp.

AccessData Certified Examiner (ACE)
Certification Date: August 26, 2008
Recertification Date: August 30, 2010

Examinations

In excess of 100 examinations of computers, cellular telephones, and other items of electronic/digital media.

EXHIBIT C
SUMMARY OF TESTIMONY OF JOSEPH BYERS

SA/CFA Joseph Byers was present during the search of Ocasio's residence and can testify as to where certain items were found. He also witnessed the initial preview done by SA/CFA Demetrio Medina.

Once the items were taken to the Computer Forensics Office at HSI, SA/CFA Byers initiated imaging of EXT1. A forensic duplicate of EXT1 was created utilizing FTK Imager.

The imaging was conducted on a SAC El Paso CCG Computer Forensics computer utilizing a Tableau Universal Serial Bus (USB) write protection device to acquire USB devices.

To insure the integrity of the acquisition, a MD5 hash value was calculated and obtained after the image was acquired. The resulting hash value was recorded and matched a verification hash calculated subsequent to the acquisition.

FTK Imager returned the following hash value for EXT1.

EXT1: 4ff4257fd3e1b0fc707569f926d32eed
Evidence Files: EXT1-EP07QR12EP0001.E01 through EXT1-EP07QR12EP0001.EQL

SA/CFA Byers also assisted on the review and testing by SA/CFA Medina.

Curriculum Vitae

Joseph Byers Senior Special Agent Computer Forensic Agent

Office Information

Department of Homeland Security
Immigration and Customs Enforcement
Office of Investigations
Special Agent in Charge
4191 N. Mesa Street, Room 217
El Paso, Texas 79902
Phone: (915) 231-3399
Cell: (915) 726-6217
Fax: (915) 231-3351
Email: joseph.byers@dhs.gov
Employment Date: 11/30/2003

Education

McNary High School
Salem, Oregon
High School Diploma

University of Texas at El Paso
El Paso, Texas
Bachelors of Business Administration- Management
Bachelors of Business Administration- Computer Information Systems

Professional Training

United States Army
23R Hawk Missile Systems Mechanic
Training Date: August 1991
Classroom Hours: 1220

Federal Law Enforcement Training Center
Immigration and Naturalization Service
Detention Enforcement Officer Basic Academy
Training Date: September 1998
Classroom Hours: 240

Federal Law Enforcement Training Center
Immigration and Naturalization Service
United States Border Patrol Academy
Training Date: September 1999
Classroom Hours: 800

Federal Law Enforcement Training Center
Criminal Investigator Training Program
Training Date: December 2003
Classroom Hours: 400

Federal Law Enforcement Training Center
U.S. Immigration and Custom Enforcement
Special Agent Training Course
Training Date: February 2004
Classroom Hours: 480

Federal Law Enforcement Training Center
U.S. Immigration and Custom Enforcement School
Asset Forfeiture Financial Investigations Course
Training Date: June 22, 2007
Classroom Hours: 80

Federal Law Enforcement Training Center
U.S. Immigration and Custom Enforcement School
Commercial Fraud Investigations Course
Training Date: March 5, 2009
Classroom Hours: 80

Prerequisite Computer Evidence Recovery Training (PCERT)
Vendor: Treasury Computer Forensics Training Program
Classroom Hours: 80
Training Date: August 21, 2007
Certificate Awarded September 26, 2007

Basic Computer Evidence Recovery Training (BCERT)
Vendor: Treasury Computer Forensics Training Program
Classroom Hours: 120
Training Date: September 5, 2007
Certificate Awarded September 26, 2007

EnCase Computer Forensics I and II
Vendor: Guidance Software
Classroom Hours: 80
Training Date: September 4, 2007
Training Date: July 19, 2010

Certificate Awarded

Forensic ToolKit Intermediate BootCamp
Vendor: Access Data
Classroom Hours: 21
Training Date: September 14, 2007
Certificate Awarded

PARABEN Cell Phone Seizure and Analysis
Vendor: PARABEN Corp.
Training Date: June 20, 2008
Certificate Awarded

PARABEN PDA Seizure and Analysis
Vendor: PARABEN Corp.
Training Date: June 20, 2008
Certificate Awarded

Forensic ToolKit Advanced BootCamp
Vendor: Access Data
Classroom Hours: 35
Training Date: July 11, 2008
Certificate Awarded

Forensic ToolKit Vista Forensics
Vendor: Access Data
Classroom Hours: 7
Training Date: July 16, 2008
Certificate Awarded

Computer Forensic Conferences
Vendor: Department of Homeland Security
Classroom Hours: 40
Training Date: September 15, 2008
Training Date: August 24, 2009
Training Date: August 17, 2010
Training Date: September 12, 2011

Professional Certifications

CompTIA A+ Certified Professional IT Technician
Certification Date: August 31, 2007
Certifying Authority: Computer Technology Industry Association

EnCase Computer Forensics I
Certification Date: September 7, 2007
Certifying Authority: Guidance Software

Forensic ToolKit Intermediate BootCamp
Certification Date: September 14, 2007
Certifying Authority: Access Data, Inc.

Paraben Certified Handheld Examiner
Certification Date: June 20, 2008
Certifying Authority: Paraben Corp.

AccessData Certified Examiner (ACE)
Certification Date: July 16, 2008
Recertification Date: July 15, 2010
Certifying Authority: Access Data, Inc.

Examinations

In excess of 90 examinations of computers, cellular telephones, Personal Digital Assistants, and other items of electronic/digital media.